

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
1 March 2001 (01.03.2001)

PCT

(10) International Publication Number  
**WO 01/15369 A1**

(51) International Patent Classification<sup>7</sup>: **H04K 1/00**,  
H04L 9/00

(21) International Application Number: PCT/US00/23312

(22) International Filing Date: 24 August 2000 (24.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
09/379,935 24 August 1999 (24.08.1999) US

(71) Applicant (for all designated States except US): **SMART TONE, INC.** [US/US]; 50 Pine Street, New York, NY 10005 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **MARK, Andrew, R.** [US/US]; 50 Pine Street, New York, NY 10005 (US).

(74) Agents: **WOODBIDGE, Richard, C.** et al.; Woodbridge & Associates, P.C., P.O. Box 592, Princeton, NJ 08542 (US).

(81) Designated States (*national*): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**

- With international search report.
- Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.



**WO 01/15369 A1**

(54) Title: SYSTEM AND METHOD OF USER VERIFICATION

(57) Abstract: This invention relates to biometric user verification in which an entered biometric feature is processed to yield an alpha numeric coded sequence representing its attributes. For increased security this coded sequence may then be encrypted in a manner specific to both the user and to the specific destination for which authorization is sought.

**Title: SYSTEM AND METHOD OF USER VERIFICATION****Inventor: Andrew R. Mark****BACKGROUND OF THE INVENTION**1. Field of the Invention

This invention relates to biometric user verification in which an entered biometric feature is processed to yield an alpha numeric coded sequence representing its attributes. For increased security this coded sequence may then be encrypted in a manner specific to both the user and to the specific destination for which authorization is sought.

2. Description of Related Art

Biometrics is the science of identifying a person through the electronic examination of his or her physical characteristics (e.g. fingerprints, voice, or retina patterns). These methods are extraordinarily useful as protections against fraud as well as an impediment to unauthorized electronic access to data networks. Biometric systems allow only those persons possessing the biological characteristic equated with them to present themselves as the authentic person in a non-face to face transaction over the telephone or a computer network.

Normally, the biometric process involves a comparison of a "live" personal characteristic with one that has been stored on a database. However, the existence of these databases provokes great concern. Not only can a biometric characteristic be used for authentication, it can be used as a tool to track and monitor a person's movements and transactions. Knowledge of such can lead to further information obtained about the person's likes, dislikes, political viewpoints, sexual habits, and health records. The use of biometric systems can therefore potentially effect Constitutionally protected areas of a person's life.

Further, each type of biometric used brings with it its own special variances and features that must be taken into consideration. For example, many voice verification systems used "hidden Markov models" (HMMs) to identify the speech

pattern of a particular person. HMMs relate to very detailed features or nuances of an individual's speech pattern. However, their use increases the rate of false rejections of an authentic user because a person's voice pattern changes according to, among other things, health and mood.

5           Therefore, for useful voice verification to take place, it becomes necessary to reduce the specificity in analysis of an entered biometric characteristic -- but in a manner that does not diminish the system's security and effectiveness. Further, it is highly preferable to the users that a biometric system operates in a manner that can accommodate privacy interests. The present invention fulfills these goals.

10

### **SUMMARY OF THE INVENTION**

The present invention performs cursory analysis of a user's inputted biometric characteristic for authentication. It compensates for any loss of security by incorporating a user device into its functioning that transmits dynamically changing  
15   device identity data to a platform. In the preferred embodiment, the invention authenticates a user's own special device as well as the user's voice pattern, thus reducing the need for high levels of specificity in voice verification.

These and other features of the invention will be more fully understood by reference to the following drawings.

20

### **BRIEF DESCRIPTION OF THE DRAWINGS**

Fig. 1 is a graphic representation of the relationship of the desired level of security as a function of the number of security measures employed.

Fig. 2 is a flowchart depicting the present invention's processing of inputted  
25   speech for both the initial approval of a password and the subsequent use of that spoken password in verifying the speaker.

Fig. 3 is a front view of a control panel of the preferred embodiment of the present invention.

Figs. 4, 5 and 6 are charts each illustrating an utterance of a spoken password  
30   and the resulting code sequences generated by the preferred embodiment of the present invention.

Fig. 7 is a chart illustrating the determination of the identification number by the preferred embodiment of the present invention.

Figs. 8A, 8B and 8C are tables illustrating the determination of code parameters which are defined for ranges of three attributes of inputted speech.

5 Fig. 9 is a chart illustrating the correspondence between the phoneme identification number determined by the preferred embodiment of the present invention and the spoken phoneme.

Fig. 10 is a block diagram indicating an alternative embodiment of the present invention in which additional levels of encryption occur prior to the User ID being  
10 received by the ultimate destination.

### **DETAILED DESCRIPTION OF THE INVENTION**

During the course of this description, like numbers will be used to identify like elements according to different figures which illustrate the invention.

15 It is well known in the security art to employ one or more of the following elements in designing a security system: (1) require the user seeking access to have some physical object (e.g., a door key), (2) require the user to have knowledge of a code or password (e.g., a PIN number to access his bank account information), and (3) require that a biometric physical characteristic of the user match a stored model of  
20 that user's characteristic. In combining these elements, a high level of security can be attained.

An important feature of the present invention is that both the biometric element and the physical object (a user device) are converted into coded sequences. Accordingly, the only stored data that are used as models for the verification  
25 comparison are these codes. Thus, a high level of security is achieved and the user's privacy interests are protected.

In addition, this combination of two different types of data permits the present invention to offer different levels of security. Reliance on device data alone will provide adequate level reliability for authentication. A combination of the two types,  
30 with a greater portion coming from the user device, would provide medium security. Alternatively, a combination of the two, with a greater portion of data extracted from the biometric, would provide high level security. Variations on these combination

levels could provide an increased number of security levels. Further, as depicted in Fig. 1 with respect to the preferred embodiment of the preferred invention, additional device features could be employed to further increase the level of security attained.

In the preferred embodiment, the present invention utilizes a user's voice as the biometric. The invention performs cursory analysis of a person's voice pattern for authentication. That is, this analysis is not as critical as conventional methods such as HMM analysis. Consequently, it is less likely in the present invention that a given user will be falsely rejected. The present invention compensates for any loss of security by incorporating a user device that transmits dynamically changing personal identification data to a platform. That is, the present invention authenticates a user's own special device as well as the user's voice pattern, thus reducing the need for high levels of specificity in voice verification.

The voice authentication process of the preferred embodiment begins with a registration phase which includes an analysis of an individual's utterances of a proposed pass-phrase. This step is performed before the phrase is ever used for authentication purposes. In one embodiment of the invention, this evaluation entails having the person speak the passphrase three times. As depicted in Fig. 2, the system (1) examines the utterance for its phonetic content and derives values based on those components; (2) Normalizes the utterance based on "System Adjustment Tones" and derives values based on these modified components; and, (3) Imposes wire-line impairments on the normalized utterance and again derives the values.

A specific example of this analysis will now be discussed in which the word "SPAGHETTI" is uttered three times. As depicted in Fig. 4, the first utterance results in a matrix of numbers. The initial "S" sound is recognized and, using a table lookup such as the one depicted in Fig. 9, this sound is quantified as phoneme ID# 29. This "S" sound is also quantified as to other parameters as well. That is, the duration, frequency range, and average volume level are similarly quantified by use of range values similar to the ones depicted in Figs. 8C, 8B and 8A, respectively. This analysis is also performed on each of the remaining phonemes that appear in the uttered word. In an alternative embodiment, these frequency and volume level range values are settable by use of system switches, as depicted in Fig. 3.

In the preferred embodiment the system next performs the same analysis for each phoneme after determined adjustments are applied to the speech signal ("Normalization"). Examples of such adjustments are background noise and type of microphone. Fig. 3 illustrates an alternative embodiment of the invention in which these parameters are either enabled or disabled by use of simple switches.

In the preferred embodiment, a third analysis is then performed for each phoneme based upon the above Normalized utterance further modified by wireline impairments. Examples of such impairments include identification of cellular versus wireline communication. Fig. 3 again illustrates an alternative embodiment wherein these impairments are selected by use of switch mechanisms.

Fig. 4 illustrates the effects of the Normalization process and the addition of wireline impairments on both the speech pattern to be analyzed and the resulting quantified values obtained. It further illustrates an important feature of the present invention. The values obtained for certain phonemes change as the speech pattern to be analyzed is modified in the manner described above. Conversely, certain phonemes are resilient to these variations. These latter phonemes are candidates to be included within an identification number to be used to identify this user.

The above analysis which related to the user's first utterance of the password "SPAGHETTI" is then repeated for the second and third utterance of this word, as depicted in Figs. 5 and 6, respectively. The summary of the results obtained for all of the utterances is displayed in Fig. 7. It can readily be seen that a phoneme that was characterized as resilient in one utterance (e.g., "E" in the 1<sup>st</sup> utterance) was not deemed so in another utterance (e.g., "E" in the 2<sup>nd</sup> utterance). The identification number for this user is obtained by utilizing only those phonemes which were deemed resilient in all three of the utterances.

That is, the system examines all the derived values and determines which values are consistent among each of the three versions and are therefore the most reliable information for authentication purposes. Inconsistent values will be ignored. Any remaining consistent values are strung together to form an identification number. Specifically, the codified phoneme ID#s, durations, and frequency values are appended to yield such an identification number, in this example, 27-B-05-01-A-01-15-E-08.

Should the system not yield sufficient resilient phonemes, the user would be directed to select a different candidate pass-phrase. Once the system determines that the resulting number is sufficiently robust for identification purposes, it notifies the user that the chosen pass-phrase is acceptable for use as an identifier in an authentication. That is, the system determines that the distinctive elements present in the proposed pass-phrase will be discernible regardless of the alterations which may be imposed on it during normal usage (such as type of microphone, background noise, etc.).

In the preferred embodiment, once this evaluation is complete, a user may perform a voice authentication with any destination. As depicted in Fig. 2, when the user makes the connection to the State Machine platform of the present invention (a non-secure state machine), a voice prompt will ask the user to speak the same pass-phrase with which the user registered. When the platform hears the same utterances by the user, it should decode the utterance into the same bracketed results as during registration. The likelihood of the appearance of the same robust phoneme selections, cadences, frequency ranges and relative phoneme levels in combination with full word text recognition provides an excellent, high-security means of user specific verification.

After the person speaks the passphrase into a microphone or other input device, the platform, as during the evaluation process, shall break down the sentences into syllables and assign values to the phonetic components (phonemes) as it did during registration. In the embodiment depicted in this example, these components include: (1) an identification number for each syllable; (2) a value for the duration of each syllable; (3) values for the frequency ranges of the syllables; (4) values for average volume of the phonemes; and, (5) a ranking of the frequency levels. Alternative embodiments, both in the speech area and relating to other biometrics permit variations in the number of such elements to be considered thereby achieving corresponding variations in the level of security attained.

The result is a number string that represents a person's voice pattern as alphanumeric values. The State Machine (STI) then encrypts the number string with a special algorithm used only for that particular destination and that particular user. In the preferred embodiment, this result is then transmitted to the end destination which then re-encrypts the number string a second time. This second encryption produces the

identification values that the destination uses to authenticate a person as the person he or she claims to be.

If the destination system has no record of the identification values being transmitted, the destination will perform a manual authentication which requires the person to input personal information to identify the person as someone authorized to make any transaction. When the destination recognizes the person, it will equate the identification number with that person.

In the future, when the values delivered match what the destination has recorded as an authorized person's values, an authentication may take place. If they do not match, access to the destination's system would be denied to the user. If the values presented are notably similar to the values on record, yet not identical, the system could request personal information from the user via voice prompt (social security number, date of birth, etc.) which would provide the extra security to allow the transaction to be completed.

In the preferred embodiment, additional security is provided by having the individual access the State Machine through a user device which transmits a dynamic signature. Such a device is described in U.S. Patent 5,583,933 issued to Applicant, Andrew Mark, on December 10, 1996, which patent is hereby incorporated by reference. Such a device is designated "SmartKey" in Step 1 of Fig. 10. In the preferred embodiment this dynamic signature is combined with the alpha numeric voice string and the result, when encrypted for the intended destination, creates a device specific user identification number (DSUID). This DSUID provides a high level of security by minimizing the likelihood of a false verification occurring. Further, the DSUID makes it very difficult for the specific user to be monitored as to other transactions he conducts independent of those performed at this destination. This maintenance of user confidentiality is an important feature of the present invention.

The user device provides yet an additional feature. It generates specific tones and transmits these tones as a reference signal to thereby be used by the State Machine to normalize the communication channel. That is, by analysis of a received reference signal, the system can adjust for various communication channel variations such as,

but not limited to, type of microphone and type of communication path (e.g., cellular versus wireline).

By way of summary the preferred embodiment of the present invention contains the following elements:

5 A. A State Machine

a. that acts as a user-specific utterance evaluator which determines upon registration:

- 10 (i) If a proposed utterance can produce consistent and reliable values repeatedly derived from the phonetic composition of the utterance (i.e., it contains robust elements which can survive impairments caused by voice channel transmission and their subsequent normalization so that the same values may be derived from them reliably over time);
- (ii) Whether the impaired iterations contain the same phonetically identifiable elements as the unimpaired elements; and,
- 15 (iii) If all the modified and unmodified utterances of the user's proposed pass-phrase derive the same values;

AND

b. which during every authentication:

- 20 (i) Normalizes the communication channels to eliminate transmission (including microphone and line) variances;
- (ii) Evaluates the utterances into phonetic elements (identifies phonemes, bracketed frequencies and duration levels); and
- (iii) Converts identified elements into numerical coefficients;

B. A destination specific encryption of the derived device ID; and,

25 C. A numeric description of the user which is destination specific.

An alternative embodiment of the present invention uses the automatic number identification (ANI) capability of the phone system to identify the number of the calling party. Such a capability is well known and includes the ability to identify the particular phone used when it is serviced by a local or private telephone switching  
30 system. In this alternative embodiment, at registration a user can elect to have the ANI number of his home or business phone used in place of the code generated by his "SmartKey". The system simple combines the ANI number to create the DSUID to be

used for identification. In this embodiment access to the system from a "foreign phone" would require use of the individual's SmartKey.

A yet another alternative embodiment of the present invention is depicted in Fig. 10 in which an additional level of encryption occurs at Step 3. This additional  
5 encryption still further protects the identity of the user and the security of any transactions he performs at other destinations. That is, the encrypted user ID received in Step 4 identifies the user to that particular destination. Even if an interloper attains the actual identity of the user associated with that destination ID, without knowledge of the encryption which occurs at each level, he cannot use this destination ID to track  
10 or monitor transactions of the user at other destinations.

While the invention has been described with reference to the above alternative embodiments thereof, it will be appreciated by those of ordinary skill in the art that various modifications can be made to the structure and function of the individual parts of the system without departing from the spirit and scope of the invention as a whole.

**I CLAIM:**

1. A security method for verifying the identity of an individual seeking access to a destination, said method using at least one inputted biometric characteristics of that individual, comprising the steps of:

5       receiving said at least one inputted biometric characteristics, each characteristic having a plurality of elements associated with it;  
      assigning values to a predetermined subset of said elements; and,  
      converting said assigned values into an identification number.

10       2. The method of claim 1 further comprising the steps of:  
      encrypting of the identification number in a manner that is specific to the destination;  
      transmitting said encrypted identification number to the destination; and,  
      authenticating the identity of the individual at the destination by determining  
15       whether there exists a previous record of the transmitted encrypted identification number in a destination data base.

      3. The method of claim 2 wherein the authenticating step further comprises the steps of:  
20       performing manual verification of the identity of the individual by an operator in the event no previous record of the transmitted encrypted identification number exists; and,  
      adding the transmitted encrypted identification number to the destination data base.

25       4. The method of claim 3 wherein only one biometric characteristic is inputted and that biometric characteristic is the individual's voice pattern contained in a pass-phrase spoken by the individual.

30       5. The method of claim 4 wherein the elements associated with the voice biometric is chosen from the group consisting of phoneme duration, phoneme frequency, and phoneme volume level.

6. The method of claim 5 wherein, prior to its use in said authentication step, the pass-phrase spoken by the individual is selected from a set of one or more proposed pass-phrase spoken by the individual.

5

7. The method of claim 6 wherein said each spoken proposed pass-phrase is evaluated by assigning values to said elements in the original spoken pass-phrase and in altered versions of that spoken pass-phrase to determine distinctive elements present in the proposed pass-phrase that will be recognizable regardless of impairments which may be present during spoken inputting of that pass-phrase.

10

8. The method of claim 7 wherein said impairments comprise background noise, variations in microphone type and quality, and variations in cellular or wireline transmission quality.

15

9. The method of claim 8 further comprising the steps of:  
receiving a identification string identifying a device used by the individual;  
and  
incorporating said identification string in the identification number.

20

10. The method of claim 9 wherein said incorporating step combines the identification string with the identification number to thereby yield the minimal amount of data required to attain the desired security sought.

25

11. The method of claim 10 wherein said authentication step is performed after a second encryption is performed upon the identification number.

12. The method of claim 11 wherein the identification string is the automatic number identification ANI of the user's phone.

30

13. The method of claim 11 wherein the identification string is a dynamic signature alpha-numeric string transmitted from a transmitter used by the individual.

14. The method of claim 13 further comprising the steps of:  
receiving one or more reference signals transmitted by said transmitter; and,  
5 normalizing the received pass-phrase spoken by the individual.

15. The method of claim 3 further comprising the steps of:  
receiving a identification string identifying a device used by the individual;  
and  
10 incorporating said identification string in the identification number.

16. The method of claim 15 wherein said incorporating step combines the  
identification string with the identification number to thereby yield the minimal  
amount of data required to attain the desired security sought.

15 17. The method of claim 16 wherein said authentication step is performed  
after a second encryption is performed upon the identification number.

18. The method of claim 17 wherein the identification string is the automatic  
20 number identification ANI of the user's phone.

19. The method of claim 17 wherein the identification string is a dynamic  
signature alpha-numeric string transmitted from a transmitter used by the individual.

25 20. The method of claim 19 further comprising the steps of:  
receiving one or more reference signals transmitted by said transmitter; and,  
normalizing the received at least one inputted biometric characteristic.

21. A security method for verifying the identity of an individual seeking  
30 access to a selected destination of a plurality of destinations, said method using at  
least one inputted biometric characteristics of that individual, comprising the steps of:

receiving said at least one inputted biometric characteristics, each characteristic having a plurality of elements associated with it;

assigning values to a predetermined subset of said elements;

converting said assigned values into an identification number;

5        encrypting of the identification number in a manner that is specific to the selected destination;

transmitting said encrypted identification number to the selected destination;

and,

authenticating the identity of the individual at the selected destination by

10        determining whether there exists a previous record of the transmitted encrypted identification number in a data base contained at the selected destination.

22. The method of claim 21 wherein said selected destination is selected by the individual using vocally inputted data.

15

23. The method of claim 21 wherein said transmitting of the encrypted identification number to the selected destination does not permit use of said selected destination's data base from being used to identify the individual, or any of his associated data base records, at any of the plurality of destinations which are not the  
20        selected destination.

24. The method of claim 22 further comprising the step of generating a billing record for said transmitting the encrypted identification number to the selected destination.

25

25. An authentication gateway apparatus for verifying the identity of an individual seeking access to a selected destination of a plurality of destinations, comprising:

30        receiving means for receiving at least one biometric characteristics of the individual, each characteristic having a plurality of elements associated with it;

assigning means for assigning values to a predetermined subset of said elements;

converting means for converting said assigned values into an identification number;

encrypting means for encrypting of the identification number in a manner that is specific to the selected destination;

5       transmitting means for transmitting said encrypted identification number to the selected destination; and,

      authenticating means for authenticating the identity of the individual at the selected destination by determining whether there exists a previous record of the transmitted encrypted identification number in a data base contained at the selected  
10   destination.

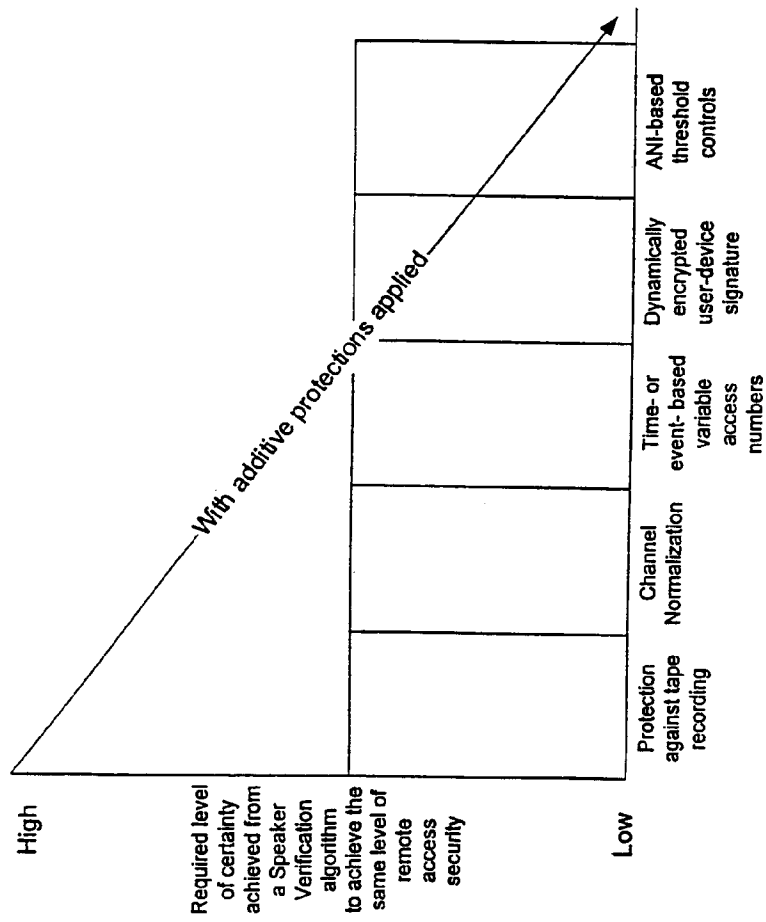


FIG. 1

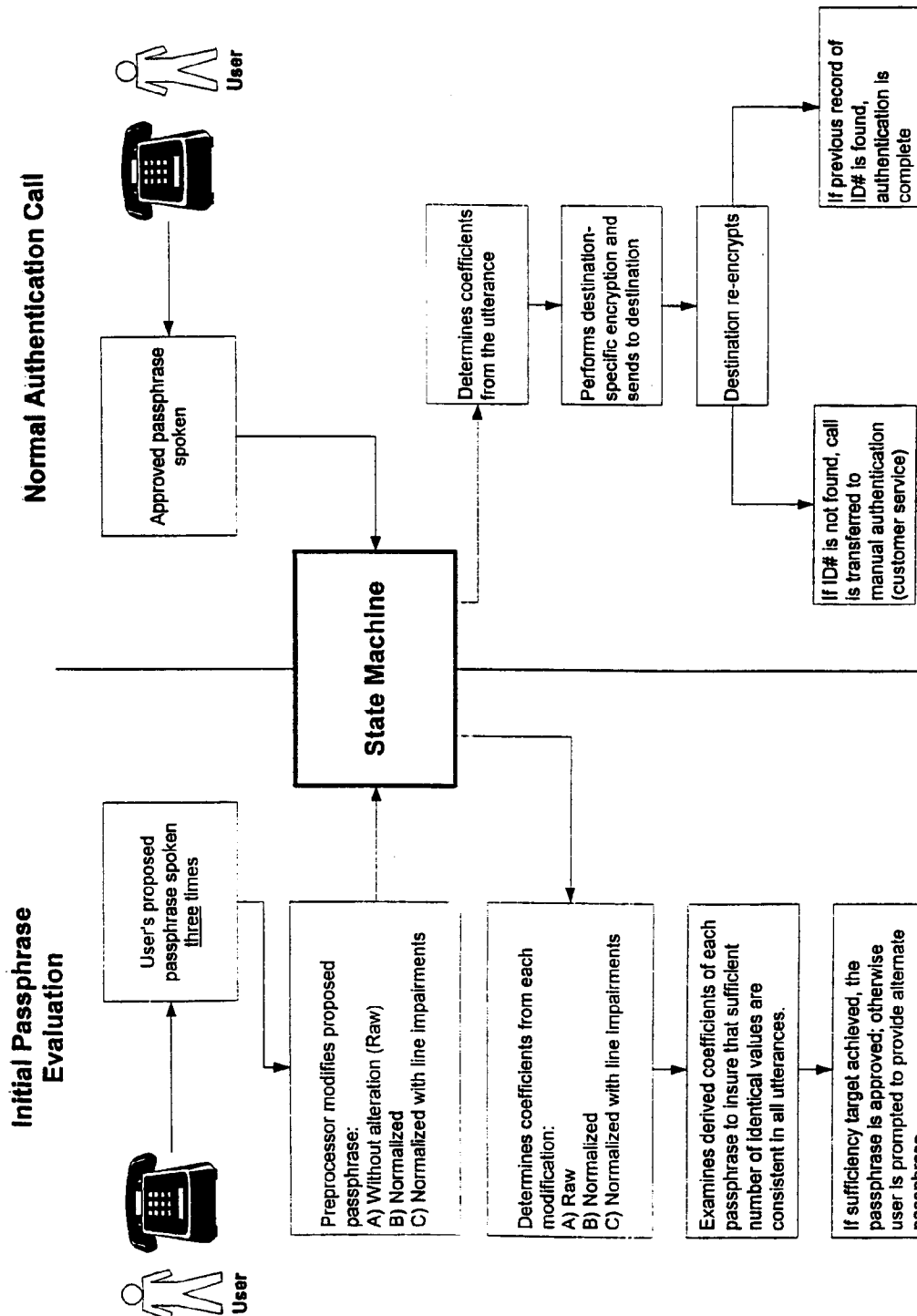


FIG. 2





<p>Input Speech File Adjustors</p>	<p>Minimum Signal Threshold</p> <div data-bbox="474 1304 662 1533"> </div>	<p>Background Noise Sensor</p> <div data-bbox="433 600 584 982"> </div>
<p>Band Limits</p> <div data-bbox="760 1262 1065 1545"> <p>HI _____ Hz      LO _____ Hz</p> </div>	<p>Microphone Type Sensor</p> <div data-bbox="837 611 985 982"> </div>	<p>Impairments To Be Applied</p> <div data-bbox="1195 772 1276 1482"> </div>

FIG. 3

Phoneme	S	P	A	G	H	E	TTI
Raw Utterance							
Phoneme ID#	29	27	1	15	16	11	31
Bracketed Duration	A	B	A	E	E	F	F
Bracketed Freq. Range	4	5	1	8	7	5	4
Avg. Bracketed Level	V	W	X	Y	Z	V	W
Level Ranking	1	3	5	6	7	2	4
Normalized (Based on SAT's)							
Phoneme ID#	29	27	1	15	16	11	31
Bracketed Duration	A	B	A	E	F	F	F
Bracketed Freq. Range	5	5	1	8	8	5	4
Avg. Bracketed Level	V	W	X	Y	Z	V	W
Level Ranking	1	3	5	6	7	2	4
With Wireline Impairments (On Normalized File)							
Phoneme ID#	29	27	1	15	16	11	31
Bracketed Duration	A	B	A	E	F	F	F
Bracketed Freq. Range	5	5	1	8	8	5	4
Avg. Bracketed Level	V	W	X	Y	Z	V	W
Level Ranking	1	3	5	6	7	2	4
Resilient/Robust Attributes of the 1st Utterance							
Phoneme ID#	29	27	1	15	16	11	31
Bracketed Duration	A	B	A	E	F	F	F
Bracketed Freq. Range	5	5	1	8	7	5	4
Avg. Bracketed Level	V	W	X	Y	Z	V	W
Level Ranking	1	3	5	6	7	2	4
Phoneme ID#	27	1	15	11	31	F	4
Bracketed Duration	B	A	E	F	F	4	W
Bracketed Freq. Range	5	1	8	7	5	4	4
Level Ranking	3	5	6	2	4	4	4

\*NOTE: This phoneme set is not used due to inconsistencies among Raw, Normalized and Impaired Sets.

FIG. 4

Phoneme	S	P	A	G	H	E	TTI
Raw Utterance							
Phoneme ID#	29	27	1	15	16	11	31
Bracketed Duration	B	B	A	E	E	G	F
Bracketed Freq. Range	4	5	1	8	7	5	4
Avg Bracketed Level	V	W	W	W	X	Y	Z
Level Ranking	1	2	3	4	5	6	7
Normalized (Based on SATs)							
Phoneme ID#	29	27	1	15	16	11	31
Bracketed Duration	A	B	A	E	E	F	F
Bracketed Freq. Range	4	5	1	8	6	6	4
Avg Bracketed Level	V	W	W	W	X	Y	Z
Level Ranking	1	2	3	3	4	6	7
With Wireline Impairments (On Normalized File)							
Phoneme ID#	29	27	1	15	16	11	31
Bracketed Duration	A	B	A	E	E	F	G
Bracketed Freq. Range	5	5	1	8	6	5	4
Avg Bracketed Level	V	W	W	W	Y	Y	Z
Level Ranking	1	2	3	4	5	6	7
Resilient/Robust Attributes of the 2nd Utterance *							
Phoneme ID#	27	1	15	15	16	11	31
Bracketed Duration	B	A	E	E	E	F	G
Bracketed Freq. Range	5	1	8	8	6	5	4
Level Ranking	2	3	4	4	5	6	7

\*NOTE: This phoneme set is not used due to inconsistencies among Raw, Normalized and Impaired Sets.

FIG. 5

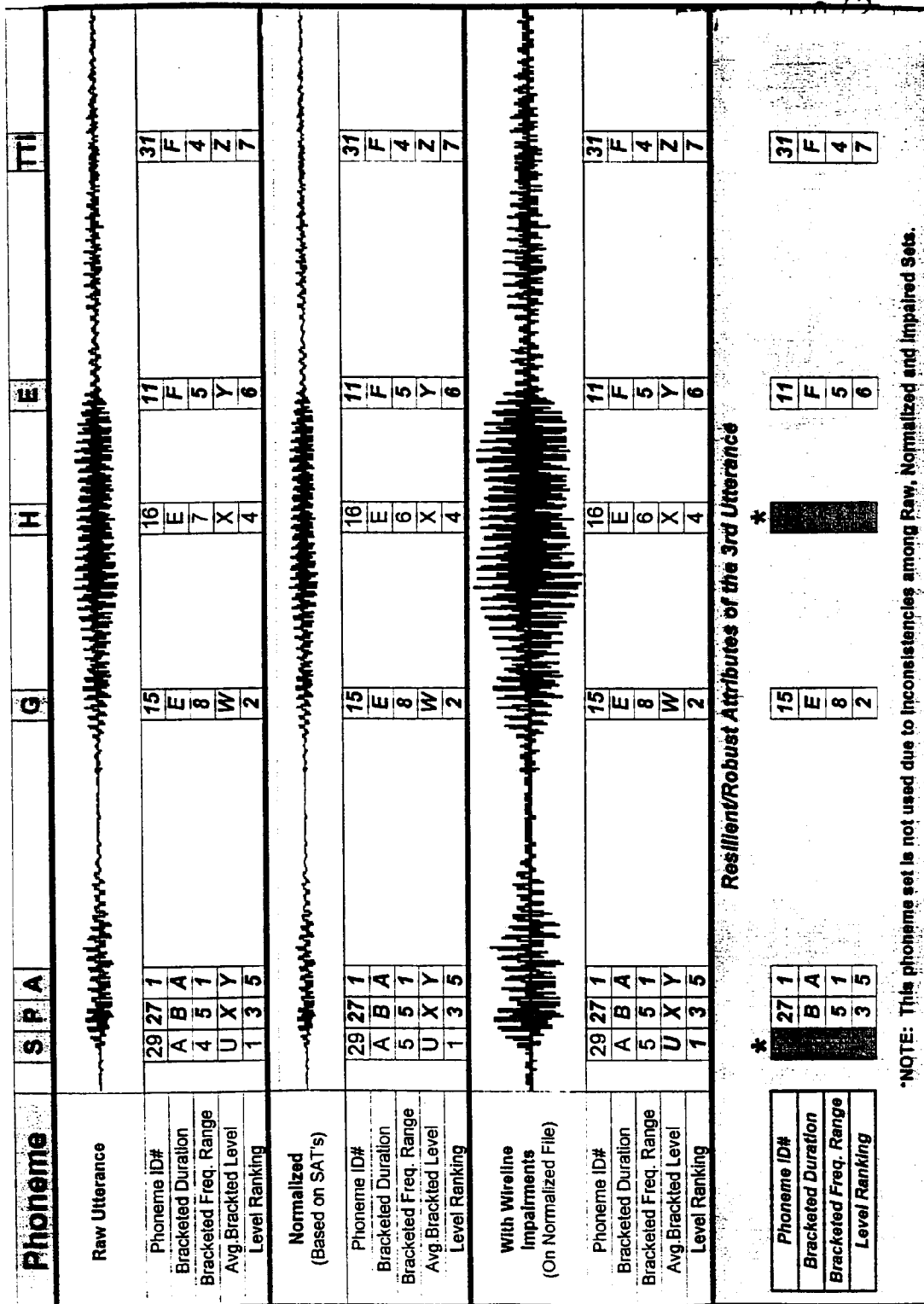


FIG. 6

Phoneme		S	P	A	G	H	E	TTI
Used in Wav.File			YES	YES	YES			
Resilient/Robust Attributes of the 1st Utterance	Phoneme ID#		27	1	15		11	31
	Bracketed Duration		B	A	E		F	F
	Bracketed Freq. Range		5	1	8		5	4
	Level Ranking		3	5	6		2	4
Resilient/Robust Attributes of the 2nd Utterance	Phoneme ID#		27	1	15			
	Bracketed Duration		B	A	E			
	Bracketed Freq. Range		5	1	8			
	Level Ranking		2	3	4			
Resilient/Robust Attributes of the 3rd Utterance	Phoneme ID#		27	1	15		11	31
	Bracketed Duration		B	A	E		F	F
	Bracketed Freq. Range		5	1	8		5	4
	Level Ranking		3	5	2		6	7
Common Resilient Attributes of ALL Three Robust Utterances during Training Session	Phoneme ID#	27 - 01 - 15					P. / US	
	Bracketed Duration	B - A - E					00 / 23	
	Bracketed Freq. Range	05 - 01 - 08					312	
Resulting Wav.File Identification #: 27-B-05-01-A-01-15-E-08								

FIG. 7

Values of Bracketed Levels		
Code	Average dBm Over Segment	
	Maximum	Minimum
Z	<-20.5	
Y	<-17.5	>-20.49
X	<-12.5	>-17.49
W	<-7.5	>-12.49
V	<-2.5	>-7.49
U	0	>-2.49

FIG. 8a

Values of Bracketed Frequency Range (Hz)			
Code	Begin Freq. Range		End Freq. Range
	Minimum	Maximum	Maximum
1	300		600
2	601		900
3	901		1200
4	1201		1500
5	1501		1800
6	1801		2100
7	2101		2400
8	2401		2700
9	2701		3000
10	3001		3300
11	3301		3600

FIG. 8b

Values of Bracketed Duration (ms)		
Code	Begin/End ms	
	Minimum	Maximum
A	40	80
B	81	120
C	121	160
D	161	200
E	201	240
F	241	280
G	281	320

FIG. 8c

9 / 10

Phoneme ID Values			
#	Phoneme	Example	Translation
1	AA	odd	AA'D
2	AE	at	AE'T
3	AH	hut	HH'AH'T
4	AO	ought	AO'T
5	AW	cow	KAW
6	AY	hide	HH'AY'D
7	B	be	BI'Y
8	CH	cheese	CH'IZ
9	D	dee	DI'Y
10	DH	thee	DH'Y
11	EH	Ed	EH'D
12	ER	hurt	HH'ER'T
13	EY	ate	EY'T
14	F	fee	FI'Y
15	G	green	GR'Y'N
16	HH	he	HH'Y
17	IH	It	IHT
18	IY	eat	IY'T
19	JH	gee	JH'Y
20	K	key	KI'Y
21	L	lee	LI'Y
22	M	me	MI'Y
23	N	knee	NI'Y
24	NG	ping	PIH'NG
25	OW	oat	OW'T
26	OY	toy	TO'Y
27	P	pee	PI'Y
28	R	read	RI'Y'D
29	S	sea	SI'Y
30	SH	she	SHI'Y
31	T	tee	TI'Y
32	TH	theta	THEY'TAH
33	UH	hood	HH'UH'D
34	UW	two	TU'W
35	V	vee	VI'Y
36	W	we	WI'Y
37	Y	yield	YI'LD
38	Z	zee	ZI'Y
39	ZH	seizure	SI'YZHER

FIG. 9

10 / 10

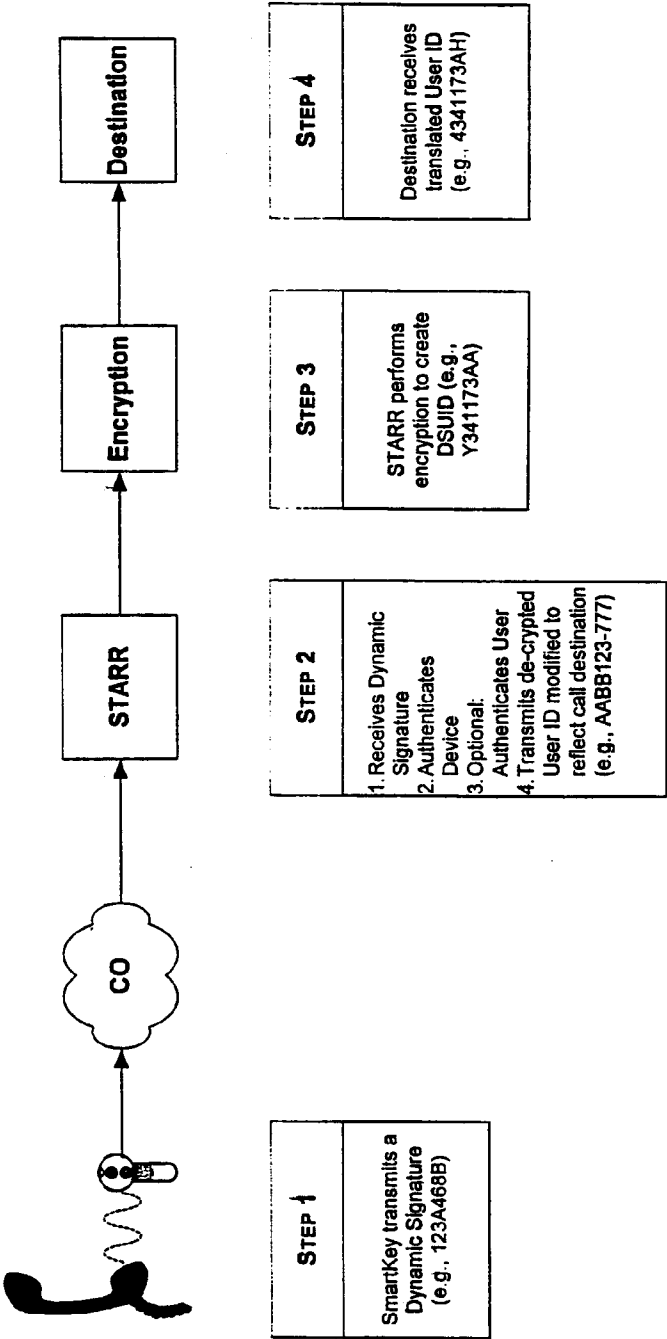


FIG. 10

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/US00/23312

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04K 1/00; H04L 9/00  
US CL : 713/182

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
U.S. : 713/182-186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,534,855 A (SHOCKLEY et al.) 09 July 1996	1
---		--
Y		4
Y	US 5,548,647 A (NAIK et al.) 20 August 1996	4
Y	US 5,636,282 A (HOLMQUIST et al.) 03 June 1997	1-25
Y	US 5,787,154 A (HAZRA et al.) 28 July 1998	1-25
A	US 5,153,918 A (TUAL) 06 October 1992	1-25
A	US 5,280,527 A (GULLMAN et al.) 18 January 1994	1-25

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier application or patent published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

02 October 2000 (02.10.2000)

Date of mailing of the international search report

27 DEC 2000

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks  
Box PCT  
Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

Gail O. Hayes *James R. Matthews*

Telephone No. (703) 306-5538